AUTHENTICATION [redacted] DATA SECURITY SYSTEM FOR [redacted]MMUNICATIONS

ABSTRACT

This invention is a dynamic parameterized context dependent cryptosystem, for general security and privacy of a communication vis-a-vis outsiders, while also limiting the access of a third party involved in the communication to selected portions of the communicated information, on a need-to-know basis. The invention thus provides an authentication and data security system for communications between two or more parties. The system provides a communication key that is derived by a first party subsystem using an encryption algorithm from key data previously provided by a second party subsystem to the first party subsystem. The communication key is transmitted to the second party subsystem, which uses a decryption algorithm to check whether the communication key was derived from any of various key data from a previously provided data pool related to the first party. The "communication key" is a mathematically derived form of a data context. It is self-encrypted in that no external keys, whether secret or public, are involved in the process.